


CSIS PROCEDURES: COLLECTION AND MANAGEMENT OF DISCOVERABLE DATASETS

SECRET

	Governing Policy: Conduct of Operations (pending the publication of the CSIS Policy on Collection, Analysis, Reporting and Retention)	
	Effective Date: 2016-08-26	Approved by: ADE
	Policy Centre:	File No:
	Version: 1	French version
	Replaces: New Policy	

1. INTRODUCTION

- 1.1 This procedure outlines requirements associated with the collection, use, and management of non-warranted discoverable datasets in support of the Service's s.12 and s.15 operational mandate.
- 1.2 This procedure does not govern the acquisition, use, or management of immediately reportable or referential datasets.
- 1.3 This procedure should be read in conjunction with the DDO Directive on Long Term Operational Data Retention. Refer to CSIS Guidelines: Identification and Collection of Datasets for additional information.

2. DATASETS

- 2.1 A dataset is a collection of information structured as an electronic record composed of searchable data elements.
 - 2.1.1 Information collected in formats that are not structured as electronic records, which are converted into a form to allow for targeted searches and advanced data analytics prior to ingestion by the datasets, and subject to the requirements of this procedure. are considered

Immediately Reportable Datasets

- 2.2 Certain datasets, considered immediately reportable, may be collected and published in support of investigations, where the nature of the data is such that it directly relates to a subject of investigation or where the nature of the data is directly indicative of threat-related activities.

- 2.2.1 Immediately reportable datasets have a significant portion of records that directly relate to a person or persons of interest, or are considered directly indicative of threat-related activities. Such datasets are to be collected and managed in accordance with the relevant policies and procedures.

CSIS PROCEDURES: COLLECTION AND MANAGEMENT OF DISCOVERABLE DATASETS

SECRET

Referential Datasets

- 2.3 Certain datasets, considered referential, provide context to facilitate the performance of the duties and functions of the Service.
- 2.3.1 Referential datasets may be acquired and used by the Service where the nature of the data is readily available to the general public
These datasets either contain no personal information (e.g.)
or are public directories, publications and business information (e.g.)
- 2.3.2 may be consulted to determine whether a dataset is referential or discoverable in nature.

Discoverable Datasets

- 2.4 Discoverable datasets are collected in support of investigations. Discoverable datasets entail a broader collection of information in which a significant portion of the data may not be related to a subject of investigation or directly indicative of threat-related activities.
- 2.5 For further information refer to the CSIS Guidelines: Identification and Collection of Datasets.

3. IDENTIFICATION OF DISCOVERABLE DATASETS

- 3.1 Discoverable datasets may be collected from a variety of sources, including by request, proactively, or via guided by CSIS policies and procedures.
- 3.2 The collection of discoverable datasets will be driven by operational requirements, determined in consultation with Branches and Regions, with a rational and demonstrable link to active targeting authorities and Intelligence Requirements.
- 3.3 Discoverable datasets are centrally managed, with eligibility for collection, access and exploitation determined by
- 3.4 All discoverable datasets identified by Service employees must be referred to to determine eligibility for collection, and, should the requirements for collection be met, ingestion into holdings and analysis.

CSIS PROCEDURES: COLLECTION AND MANAGEMENT OF DISCOVERABLE DATASETS

SECRET

- 3.5 Discoverable datasets voluntarily provided to the Service will be considered against the relevant collection authority to ensure the appropriate requirements are met. Decisions and rationale will be documented, including whether a dataset is deemed ineligible for collection, where applicable.

4. COLLECTION OF DISCOVERABLE DATASETS

- 4.1 Discoverable datasets may be collected under s.12 or s.15 of the *CSIS Act*.

Section 12 Collection

- 4.2 In order to collect a discoverable dataset pursuant to s.12, it must first be established that the information contained therein relates to activities suspected of constituting a threat to the security of Canada as defined in s.2 of the *CSIS Act*, or has operational value in relation to the investigation of such threats.
- 4.3 For s.12 collection, once the connection to the investigation of threat-related activities is established, it must be determined that the collection of the dataset is strictly necessary to the conduct of CSIS' mandate to investigate, analyze and report threats to the security of Canada.
- 4.4 To determine whether the collection is strictly necessary, the following must be established and the rationale for collection recorded:
- a) the information sought to be derived from the dataset;
 - b) how the information is expected to assist the Service carry out its mandate of investigating and analyzing threats to the security of Canada, and whether there is a demonstrable need for that information;
 - c) the information is not reasonably available through other, potentially less intrusive, means; and
 - d) it is not feasible to obtain a narrower data set.

Section 15 Collection

- 4.5 In order to collect a discoverable dataset pursuant to s.15, it must be established that the information contained therein is relevant to investigations in support of the provision of security assessments or advice to Ministers in support of their duties and functions under the *Immigration and Refugee Protection Act* and/or the *Citizenship Act*.

CSIS PROCEDURES: COLLECTION AND MANAGEMENT OF DISCOVERABLE DATASETS

SECRET

Additional Privacy Protections

- 4.6 Consideration will be given to the privacy interests attached to each dataset and the importance of the data to an investigation by evaluating the nature and volume of collection, the inclusion of non-threat related information and the nature of the threat. If the impact on privacy is disproportionate to the threat, the dataset should not be collected.

Approval Authorities

- 4.7 The collection of each discoverable dataset must be approved at the _____ level.
- 4.8 At any time, employees and managers may consult their supervisors and/or, with the approval of _____ CSIS Legal Services for additional information regarding the collection of a discoverable dataset.

5. INGESTION

- 5.1 All discoverable datasets will be appropriately classified and ingested by _____ into _____ holdings.
- 5.2 The Classification and Designation of Recorded Information may be consulted for further guidance on the appropriate level of classification for each discoverable dataset.
- 5.3 Discoverable datasets will be held by _____
- 5.4 To the extent feasible, _____ will consider the removal of extraneous fields and the anonymization of datasets.
- 5.5 _____ will maintain a catalogue of all datasets ingested into its holdings on _____
- 5.6 Each discoverable dataset will have a file number and an individual record containing the following:

CSIS PROCEDURES: COLLECTION AND MANAGEMENT OF DISCOVERABLE DATASETS

SECRET

6. EXPLOITATION

- 6.1 Exploitation of discoverable datasets will occur only in support of active investigations.
- 6.2 Access to discoverable datasets will be restricted to employees to respective discoverable datasets will be determined by Access rights of
- 6.3 Access will be monitored and reviewed, randomly and periodically, through the Service's internal audit system by Instances of non-compliance may result in disciplinary actions as per CSIS Procedures: Breaches of Conduct and Disciplinary Measures.
- 6.4 Information derived from the exploitation and analysis of discoverable datasets will be reported to the applicable investigative file, and will subsequently be managed and retained in accordance with the relevant policies and procedures.
- 6.5 To ensure the accuracy and integrity of discoverable datasets, the integrity of the original source data will be maintained. Exploitation activities will not alter the original copy.

Information Sharing

- 6.6 Discoverable datasets will not be shared with except in accordance with s.17 and s.19 of the CSIS Act. Such sharing must fall within the scopes of cooperation approved by the Minister and will be considered on a case-by-case basis by in consultation with relevant operational Branches to determine requirements and safeguards.
- 6.7 For further information on the requirements and considerations associated with information sharing, please refer to the DDO Directive On Information Sharing with Foreign Entities, DDO Update to Interim Directive for All Information Sharing Activities, OPS-509 Recording Tracking of Exchanges of Information and Intelligence, OPS-601 Authorized Disclosure of Operational Information and Intelligence, and OPS 602 Disclosure of Security Information or Intelligence.

7. REVIEW AND RETENTION

- 7.1 Information derived from the exploitation and analysis of discoverable datasets will be reported to the applicable investigative file, and subsequently managed and retained in accordance with the DDO Directive on Long Term Operational Data Retention.
- 7.2 All operational reporting derived from discoverable datasets will specify the provenance of the original dataset. The dataset from which operational reporting was derived will take on the retention period of the investigative file associated with the most recent reporting.

CSIS PROCEDURES: COLLECTION AND MANAGEMENT OF DISCOVERABLE DATASETS


SECRET

- 7.3 Discoverable datasets will be assigned a review period of _____ upon collection. Prior to the expiry of this period, _____ will conduct a review to assess the continued utility and relevance of the discoverable dataset to the conduct of the Service's mandate, the need for further retention, and designate the next review period.
- 7.4 As required, _____ will tailor the retention periods of specific discoverable datasets taking into consideration the sensitivity of the information, its ongoing utility, or the requirements of the originator.
- 7.5 If a dataset has not been used to generate operational reporting, it will be disposed of from _____ holdings if it has reached the end of its retention period or is deemed to no longer be useful or relevant. Consideration may also be given to deletion prior to the end of the retention period.
- 7.6 If a dataset has been used to generate operational reporting, but is no longer useful or relevant, it will be moved into administrative holdings, with the assigned retention period of the last investigation to have used the dataset.
- 7.7 All decisions related to review and retention will be documented, along with their rationale.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

CSIS Guidelines: Identification and Collection of Datasets

Secret

	Governing Procedure: Collection and Management of Discoverable Datasets	
	Effective Date: 2016-08-26	Approved by: ADE
	Policy Centre:	File No:
	Version: 1	French version
	Replaces: New Policy	

The following is intended to provide assistance in ensuring that collection and exploitation of datasets is in accordance with the CSIS Policy Framework, and CSIS Procedure: Collection and Management of Discoverable Datasets.

BACKGROUND

The threat environment in which CSIS functions has changed considerably since its creation. Threats evolve quickly, are complex, and may be global in scope. New technological and transmission capabilities have emerged that are used in innovative ways to obscure threat-related activities.

Operational requirements and investigatory techniques have had to adapt to address the challenges presented by the contemporary operating environment.

One such technique is the ability to exploit information contained in datasets to support authorized investigations. This capability has become critical to meeting CSIS' mandate, yielding important intelligence that is not discoverable through other means.

The collection of non-warranted discoverable datasets is governed by s.12 and s.15 of the *CSIS Act*. For s.12, the dataset must relate to activities suspected of constituting a threat to the security of Canada as defined in section 2 of the *CSIS Act*, or have operational value in relation to the investigation of such threats. It must also fit within the bounds of that which is considered strictly necessary to investigate threats to the security of Canada. For s.15, the dataset must be relevant to the provision of security assessments or advice to Ministers in support of their duties and functions under the *Immigration and Refugee Protection Act* and/or the *Citizenship Act*.

CSIS activities are also subject to the *Charter of Rights and Freedoms*. Section 8 of the *Charter* protects against unreasonable search and seizure, and applies not only to persons and property, but also to personal information. Due to the nature of dataset collection, it is not always possible to discern at the point of collection which information will be threat-related and which will not. As such, the acquisition of datasets potentially involves the collection of information that is not

Why is this type of collection different from other s.12 collection activities?

As distinct from case-specific collection, where information is collected in relation to a subject of interest, discoverable datasets collected by entail a broader collection of information in which a significant portion of the data may not be related to specific targets.

CSIS Guidelines: Identification and Collection of Datasets

Secret

threat-related, along with the necessary threat-related information. For this reason, additional controls are placed on certain datasets, including restricted access rights.

The guidance provided below will help the Service demonstrate due diligence respecting both *CSIS Act* and *Charter* considerations in the collection and exploitation of datasets.

IDENTIFICATION OF DATASETS

A dataset is a collection of information organized as structured electronic records that may be subject to targeted searches and/or advanced data analytics. The Service collects a variety of datasets in support of its duties and functions containing a wide range of information. These datasets are organized into three categories with associated collection and handling requirements.

Immediately Reportable

A dataset that is considered immediately reportable is one in which the information contained is directly linked to an individual targeting authority, or in which the majority of the information is directly indicative of threat-related activities.

Volume vs. Nature

Whether a dataset is considered discoverable or immediately reportable depends on the nature of the information contained, rather than the number of records. It is important to remember that immediately reportable datasets may contain a large volume of records, but the information is necessary to the investigation of the target.

Immediately reportable datasets may be collected in support of investigative activities and reported in as with other supporting facting information. Provided it meets other relevant policy requirements, the focused nature of the collection does not demand any additional or specific information management or retention practices beyond those safeguards built into and set out in relevant operational policies.

Referential

Referential datasets provide vital contextual information for the Service to perform its duties and functions. These datasets may be acquired by the Service where the nature of the data is readily available to the general public and contain no personal information (e.g., or are public directories, publications and business information (e.g.,

These datasets either

),

CSIS Guidelines: Identification and Collection of Datasets

Secret

Referential datasets may be made broadly available to users within the Service, and do not require the additional safeguards and protections required for the management of discoverable datasets.

To be clear, referential datasets do not include information that would tend to reveal details about

Discoverable

Discoverable datasets are necessary for the investigation of threats, but the majority of the information contained may not in and of itself be directly or immediately indicative of threat-related behaviour, or directly linked to an individual target

Discoverable datasets are collected by _____ under s.12 or s.15 of the *CSIS Act*, and must meet the respective collection thresholds.

These datasets tend to include personal information carrying privacy interests. Due to the nature of the collection, potentially involving individuals who are not, and may not ever be, engaged in any threat-related activities, additional privacy protections are put in place.

THE APPLICATION OF STRICTLY NECESSARY

Discoverable datasets collected by _____ pursuant to s.12 of the *CSIS Act* must fit within the parameters for collection set out in s.12; that is that they be strictly necessary to investigate threats to the security of Canada. The Service has developed a set of criteria to be satisfied in the interpretation of strictly necessary, which will guide the collection of such datasets. To determine if a discoverable dataset is strictly necessary to s.12 investigations, the following is to be established and recorded:

What information is sought to be extracted from the dataset?

Why do privacy interests matter when discussing datasets?

The Service has the legal authority to impact privacy interests in its investigation of threats to the security of Canada. Due to the nature of datasets containing personal information, it is possible that the majority of the individuals to whom the information relates are not, and may not ever become engaged in threat-related activities.

However, the Service must collect the entire dataset to extract the threat-related information.

This constitutes a search of these individuals' information. In these cases, the personal information of those who are not engaged in threat-related activity require additional safeguards to protect their privacy interests.

CSIS Guidelines: Identification and Collection of Datasets

Secret

How the information is expected to assist the Service carry out its s.12 mandate, and whether there is a demonstrable need for that information?

Is the information available through other, potentially less intrusive means?

Could a narrower dataset be collected?

SECRET
2015 11 24

MEMORANDUM

TO: DDO

CLASSIFICATION: SECRET

FILE(S):

c.c. ADE
ADC

FROM: Chief, DDO Secretariat

DATE: 2015 11 24

SUBJECT: Clarifications to the DDO Directive on Long-Term Operational Data Retention relative to the retention and processing of non-warranted imagery.

EXECUTIVE SUMMARY

On 2014 09 26, the DDO Directive on Long-Term Operational Data Retention was issued to provide direction on retention of information collected under Sections 12, 15 and 16 of the *CSIS Act*. This DDO Directive introduced, among other things, a third category of information (or data) to more effectively support the retention of non-warranted imagery (e.g.).

and have since raised concerns regarding the application of this DDO Directive as it pertains to the data

DISCUSSION

Based on consultations with the following clarifications to the DDO Directive on Long-Term Operational Data Retention are proposed:

1. In the exercise of determining whether non-warranted imagery is *potentially exploitable*,

RECOMMENDATION

DDO approval is sought to issue the clarifications to the DDO Directive on Long-Term Operational Data Retention, as described above.

DDO Secretariat

APPROVED:

Deputy Director Operations

2015 11 24

SECRET

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

DDO Directive on Long-Term Operational Data Retention

2014 09 26

The purpose of this Directive is to provide direction on retention of information collected under Sections 12, 15 and 16 of the *CSIS Act*. This Directive supersedes the 2012 03 01 *DDO Directive on Retention of information collected under ss. 12, 15 and 16 of the CSIS Act*. It introduces a third category of information¹ (or data) to more effectively support the retention of non-warranted imagery (e.g.), and other non-warranted technical information (); and clarifies the regime under which all employees involved in the collection and retention of operational data must operate. It also accommodates necessary changes imposed upon us through the implementation of the project.

All collected information falls into one of three categories:

Unpublished: Formerly referred to as “not reported”. *Unpublished* information is data or material that is not found to have any intelligence value within one year of collection and is destroyed. Unless identified as *Potentially exploitable* or *Published* (see below), all data collected into Service holdings will by default be *Unpublished* and will be subject to destruction after one year.

Potentially Exploitable: This category is meant to identify material from non-warranted technical tools (primarily non-warranted imagery , which has not been *Published* by a Service employee within one year and may still be operationally relevant. Information categorized as *Potentially exploitable* will be retained according to the CSIS Retention Schedule (CRS)².

Published: Formerly referred to as “reported”. *Published* information is any data or material that forms part of, or is used in the preparation of, a report (e.g.). *Published* also includes any data or material that is found to be relevant under ss. 12, 15 or 16 of the *CSIS Act* and is tagged, referenced or otherwise manipulated in . Data that is used to create a report will be subject to the CRS. (Note that s. 16 data will continue to be retained for one year, as per the CRS.)

Warranted Collection

This Directive does not change the retention scheme applied to material or information collected pursuant to s. 21 of the *CSIS Act* warrants. Information collected under warrant is still subject to the retention schedule outlined in the warrant. Generally, these retention schedules are specified in Conditions 2 and 3, which provide for the destruction of unreported

¹ See Appendix 1 for the definition of “Information”. In this Directive, the terms “information” and “data” are used interchangeably.

² The disposition of the Service’s records is managed by the Library and Archives of Canada Act.

in accordance with the

DDO Directive on Long-Term Operational Data Retention

2014 09 26

information. If in doubt regarding the interpretation of these or any other warrant conditions, DLS must be consulted.

Table 1: Summary of Retention Categories

Collection Authority	Default Retention Category	Published Retention Period
	(Retention period) ³	(Retention Period)
General collection authority	Unpublished	CRS
S.16 collection authority	Unpublished	
	Unpublished	CRS
S.15 collection authority	Unpublished	CRS
S.12	Potentially exploitable	CRS
Warranted	Unpublished (subject to warrant conditions)	CRS

Application examples:

Examples are provided in Appendix 4, below.

Exculpatory Information

³ CRS date ranges are provided for illustrative purposes only.

_____ is responsible for the application of the Service's information management lifecycle and for the final disposition of records in accordance with the *Library and Archives of Canada Act*. Each type of record (ex: S12-Investigation; S12-Warrant; S15-Government Screening, etc.) has a different lifecycle before final disposition. Please consult with _____ for up-to-date records management information.

DDO Directive on Long-Term Operational Data Retention

2014 09 26

Incidentally Collected Information

Any *Published* s. 12 or s. 15 information collected incidentally under a s. 16 collection authority (under warrant or not) must be retained according to the applicable s. 12 or s. 15 retention schedules, or as per warrant conditions. In case of disagreement, the warrant conditions prevail.

Metadata and Datasets

This Directive does not apply to metadata or datasets received by branch, with the exception of metadata associated with solicitor-client communications. In cases of solicitor-client communications, applicable procedures must be followed and if it is determined that the communication must be destroyed, its associated metadata will also be destroyed. Please consult the CSIS Glossary of Terms and Definitions, available on the CSIS webpage, for the definition of *metadata*.

Legal Hold

In cases where the Service collects information that may be relevant to a legal proceeding, a security certificate or certain security screening procedures (government or immigration), data collected in relation to a particular individual must be retained until the final disposition of the proceeding. Information retained under this authority will be assigned *legal hold* status.

Legal hold is not an information retention regime. Legal hold status overrides the three information retention categories described above. All collected information placed under legal hold must be retained for as long as the legal hold is in force. When legal hold is removed, the information reverts to the applicable retention regimes as per the CRS.

HQ Operational DGs, in consultation with DG and DLS, are responsible for determining if information on an individual subject of Service investigative or collection authorities must be placed in legal hold. In making determinations, the following criteria must be considered:

DDO Directive on Long-Term Operational Data Retention

2014 09 26

Once a determination has been made, the DG must clearly communicate this decision to the employees concerned, specify the date on which the retention of all information begins, and document this decision on the appropriate file. The decision must also be communicated to the unit. The DG who made the

determination will be responsible for re-assessing the relevance of the legal hold on a yearly basis. The fact that a source is subject to a legal hold will be indicated in the invocation message for the specific tool or technique.

Please see Appendix 2 for more detailed procedures related to legal hold determinations.

Data collected from a source identified as having *legal hold* status will remain so until the legal hold is lifted. Once the legal hold is lifted, any data collected will revert to its default state (either unpublished, unpublished, or potentially exploitable).

Coming Into Force

This Directive will come into force on 2014 12 01.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

DDO Directive on Long-Term Operational Data Retention

2014 09 26

Appendix 1: Definitions

For the purpose of this Directive, the words "information" or "data" includes but is not limited to:

- Any document, information, object, image, record or communication obtained under a warrant, pursuant to sections 12 and 21 of the Act,
- Any material obtained during section 12 (non-warranted) or section 15 investigations,
- Any original handwritten notes made during an interview, a meeting, or a surveillance operation,

When it is not possible to make written operational notes during the event at which the information is acquired, those notes should be made as soon as possible after the event, or a report of the information must be entered in the Service's database as soon as possible.

- *Operational notes* include any rough draft, first draft, drawing, diagram, calculation, audio or video recording, any photograph or information saved on an electronic medium, or any other document produced by an employee that is used to prepare a report for the Service.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

DDO Directive on Long-Term Operational Data Retention

2014 09 26

Appendix 2 – Procedures related to Legal Hold Determinations

Once an HQ DG makes a determination that an individual is subject to a legal hold, that determination will be sent to the relevant (or designate) who, in consultation with will collate all of the technical source numbers that are currently collecting against the target. Once the list is compiled:

1. The will send the complete list to and to the relevant
2. will instruct relevant units within the regions to take appropriate action and ensure that collection and retention systems comply with the legal hold requirement;
3. will request that an amendment be made to every (and subsequent) referring to an active technical source to reflect the fact that information obtained by the technical source is subject to a legal hold;
4. will, in coordination with the , maintain a list of targets within their areas of responsibility subject to a legal hold. When an invocation (in the form of a) is submitted, the must verify whether the target is subject to a legal hold or not. A note will be added to the if the target is subject to a legal hold. Once the is approved, and if the target is subject to a legal hold, the will advise regional the and accordingly.
5. The will also notify the of the legal hold. Any subsequent upgrade, renewal, or termination of the target's targeting authority must indicate if the target is subject to a legal hold.

Any time an investigative tool is subject to an invocation (in the form of an), either to initiate, to renew, or to terminate the use of the tool, the requestor or the must determine if the target is subject of a legal hold. In cases where the legal hold exists, the DG who made the original determination must be consulted and must re-assess the relevance of the legal hold. The consultation with the DG who makes the determination can be conducted via e-mail and should not interfere with the regional invocation process. However, once the determination is made, it should be clearly indicated in the and communicated to appropriate personnel.

A decision to remove a legal hold will be communicated in the same manner.

and procedures will be updated to reflect this requirement.

DDO Directive on Long-Term Operational Data Retention

2014 09 26

Appendix 4 – Examples

The following examples will serve to illustrate the principles outlined in this Directive.

S.12 Collection to S.16 Published Report

1. A regional employee submits a

subject to a legal hold. receives the

The target is not

by

default, for the full amount of time permitted under CRS as *potentially exploitable* (in this case,). A from this is found to be relevant to a s. 16 collection requirement and a report is created. The sequence on which the report is based is marked “published”. Normally, “published” s. 16 data is retained for

However, since the was installed under a s. 12 targeting authority, and since the longer of the two states prevails (s. 16 *published* vs. s. 12 *potentially exploitable*), the on which the s. 16 report is based is retained for

S.16 Collection to S.12 Published Report

2. A regional employee submits a

subject to a legal hold. receives the

s. 16 collection authority. The target is not

by

default, for (*unpublished*). A from this is found to be relevant to a separate s. 12 targeting authority and a report is created. The on which the report is drawn is marked “published”. Normally, “published” s. 16 data is retained for. However, since the information is reported under a s. 12 targeting authority, and since the longer of the two *published* states prevails, the sequence on which the s. 12 report is based is retained for. The remainder of the is destroyed after

S.12 Collection on a Target Subject to a Legal Hold

3. A regional employee submits a

to a legal hold. receives the

s.12 target. The target is subject

When recorded,

is retained, by default, for the

full amount of time permitted under CRS as *potentially exploitable* (in this case,). However, because the target is subject to a legal hold, destruction of the is suspended until the legal hold is lifted.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Canadian Security Intelligence Service

Operational Data Analysis Centre

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Privacy Impact Assessment

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

i
Canadian Security Intelligence Service
Operational Data Analysis Centre
Privacy Impact Assessment

Document Change Control Table

Version	Date	Description	Author
DRAFT Privacy Impact Assessment Version 1.0	September 28, 2009	First draft of Privacy Impact Assessment Report	Consultant
DRAFT Privacy Impact Assessment Version 2.0	November 25, 2009 TBD	Revised version of Privacy Impact Assessment Report incorporating comments from ODAC reviewers.	Consultant
DRAFT Privacy Impact Assessment Version 2.1	February 25, 2010	Minor Editing	ATIP
DRAFT Privacy Impact Assessment Version 2.2	April 20, 2010	Minor Editing	ATIP
FINAL Privacy Impact Assessment Version	August 10, 2010	Final	ATIP

Table of Contents

	Page
Document Change Control Table	ii
Table of Contents	iii
Table of Figures	iv
Executive Summary	v
Foreword	viii
1.0 Introduction	1
Content and Objective of the Report	1
Scope of Work and Approach	1
Terminology	2
Reference	6
Participants	6
2.0 Business Process and Data Flow Analysis	7
Introduction	7
Background	7
Governance Structure	8
ODAC Concept	9
Applicable Legislation, Regulation and Policy	21
3.0 Privacy Analysis	23
4.0 Privacy Risk Management Plan	52
Accountability	52
Collection of Personal Information	52
Consent	52
Use of Personal Information	52
Disclosure and Disposition of Personal Information	52
Accuracy of Personal Information	53
Safeguarding of Personal Information	53
Openness	54
Individual's Access to Personal Information	54
Challenging Compliance	54
5.0 Communications	55
6.0 Conclusion	56
Appendix A -	Error! Bookmark not defined.6

SECRET

Table of Figures

Figure 1 - Organization of CSIS	9
---------------------------------------	---

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Canadian Security Intelligence Service
Operational Data Analysis Centre
Privacy Impact Assessment

Executive Summary

The Canadian Security Intelligence Service (CSIS) collects and analyzes information and security intelligence from across the country and abroad and reports to and advises the Government of Canada on national security issues and activities that threaten the security of Canada. The activities that constitute a threat to the security of Canada include:

- terrorism (serious violence for the purpose of achieving a political, religious or ideological objective);
- proliferation of weapons of mass destruction;
- espionage;
- transnational criminal activity; and
- foreign-influenced activity.

To derive more value from the data collected, the Service established an Operational Data Analysis Centre (ODAC) which was tasked with developing a data exploitation environment as well as being a centre of excellence to more rigorously exploit and analyze data collected by the Service.

It was also critical to improve the capability to process data that contains context relevant information to present to its' investigators. To this end, the concept of ODAC introduces the notion of data exploitation

ODAC is in a capacity building phase in exploiting evolving opportunities to provide greatly enhanced analytical support to operations/investigations resulting from the power, speed and sophistication of today's information technology. The information used by ODAC is covered by personal information banks; SIS PPU 015 (CSIS Records) and SIS PPU 045 (CSIS investigational Records, Exempt Bank). The objective of this report is to assess the privacy implications in this capacity building phase which involves improved exploitation and analysis of existing corporate repositories, using readily available analytical tools and better searching.

This PIA report describes the privacy-related impacts of establishing the capacity building phase of ODAC and proposes mitigation strategies for the identified privacy risks associated with it. The assessment process has identified **no high privacy risks**. The privacy-related risks highlighted in this report are of lesser magnitude (six low risk items). Those risks concern the use of personal information; accuracy of personal information; disposition and retention requirements; and safeguarding personal information.

This report reflects the business model for ODAC as of the date of the report – it is a snapshot in time and scope. As the ODAC project moves forward with implementing follow-on phases and capacity development, privacy principles and fair information practices as outlined in both the *Standards Council of Canada's Model Code for the Protection of Personal Information* and the *Privacy Act*, should continue to be designed into core program and project objectives. Appropriate development of the

Canadian Security Intelligence Service
Operational Data Analysis Centre
Privacy Impact Assessment

SECRET

privacy risk management plan detailed herein must continue, with short-term focus upon addressing

The table below summarizes the privacy risks identified through the PIA process and categorizes levels of risk as low or moderate (no high risks were identified) – defined by a factor of both impact and likelihood of occurrence. The goal of this risk management activity is to maintain privacy risks within acceptable levels. The higher ratings provide an indication of priority areas for implementing suggested risk avoidance and mitigation mechanisms.

#	Element	Nature of risk	Level of risk			Mitigating Mechanisms
			Low	Moderate	High	
1	USE OF PERSONAL INFORMATION	ODAC complies with Service's established policies and procedures.	●			Responsibility: Ensure that Service's established policies and procedures are met.
2	DISCLOSURE AND DISPOSITION OF PERSONAL INFORMATION	Retention and disposition standards are in accordance with established Service's policies and procedures.	●			Responsibility: Using a manual process ODAC disposes of information in accordance with the Service's IM policy.
3	DISCLOSURE AND DISPOSITION OF PERSONAL INFORMATION		●			Responsibility:
4	ACCURACY OF PERSONAL INFORMATION		●			Responsibility: Recommendation: Develop processes to ensure that the data stored in the ODAC environment remains in agreement with to assure integrity as it relates to authenticity, accuracy, currency and completeness.

Canadian Security Intelligence Service
Operational Data Analysis Centre
Privacy Impact Assessment

SECRET

#	Element	Nature of risk	Level of risk			Mitigating Mechanisms
			Low	Moderate	High	
5	SAFEGUARDING OF PERSONAL INFORMATION	ODAC is pioneering a new way of CSIS doing analysis – processes, data sources, IT tools.	●			<p>Responsibility:</p> <p>Recommendation: Conduct a harmonized TRA project to ascertain the risk environment with an examination of information assets and their values, as well as threats and vulnerabilities to determine the acceptability of residual risks and if necessary, identify mitigation strategies and security safeguards.</p>
6	SAFEGUARDING OF PERSONAL INFORMATION	ODAC analysts embrace the need to share concept when conducting authorized investigations.	●			<p>Responsibility:</p> <p>Recommendation: Ensure IT systems are safeguarded</p> <p>Recommendation: Develop a plan to ensure that access controls are put in place</p> <p>Recommendation: Develop a security audit regime</p>

Canadian Security Intelligence Service
 Operational Data Analysis Centre
 Privacy Impact Assessment

SECRET

Foreword

This PIA report presents privacy risks identified and mitigation/avoidance measures for action by ODAC governance bodies. The process of managing privacy risks is iterative in nature and, consequently, ongoing assessments performed at key milestones throughout the ODAC program's life cycle should identify new risks requiring ways to resolve them.

The privacy principles and fair information practices as outlined in both the Canadian Standards Associations *Model Code for the Protection of Personal Information* (CAN/CSA-Q830-96) and the *Privacy Act* should continue as core program and project objectives. An action plan identifying responsibility for addressing any unmitigated privacy risks, as well as how and when, accompanies this PIA (Section 4.0). CSIS ATIP and ODAC program representatives have consulted the Office of the Privacy Commissioner (OPC) and those consultations will continue.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Canadian Security Intelligence Service
Operational Data Analysis Centre
Privacy Impact Assessment

1.0 Introduction

Content and Objective of the Report

To derive more value from the data already collected by the Service, the Operational Data Analysis Centre (ODAC) was developed and tasked with creating a data exploitation environment as well as being a centre of excellence to more rigorously exploit and analyze the data collected. The goal of this environment is to derive new information and knowledge from the collected data to better achieve its mandate. ODAC is evolving using a phased approach based on attainable goals and the development of business tools.

The objective of this report is to:

- comply with the requirements of the TB PIA policy; and
- assess the privacy implications after the completion of the capacity building phase – improved exploitation and analysis of existing corporate repositories, readily available analytical tools and better internet searching.

This report contains information regarding the capacity building phase of the ODAC's development. A future development phase foresees

The final phase envisages a mature program. As ODAC evolves, the PIA process will also; later versions of this report will contain the privacy risks associated to the changes to ODAC's data exploitation environment and capabilities.

Scope of Work and Approach

The scope of this PIA is restricted to the business processes that access and use personal information (PI) associated with ODAC only. The collection and use of PI by other operational and analytical components of the Service are out of scope.

The methodology and approach outlined in the *TB Privacy Impact Assessment Guidelines* document formed the foundation for this PIA. The approach for completing the PIA included a review of documentation referred, as well as interviews with key stakeholders and subject matter experts. This data gathering approach allowed for summarization of the proposed business model. Furthermore, this PIA does not constitute an audit of privacy compliance mechanisms.

The process of managing privacy risks is iterative in nature and, consequently, ongoing assessments performed at key milestones throughout the ODAC program's life cycle will identify new risks and present ways to resolve them. As new information-sharing arrangements are completed, technical solutions developed, completed and new ODAC solutions ready for implementation, assessments of the potential privacy risks occurs and are added to the report. The OPC will receive updated versions of this PIA, as ODAC develops its capabilities and

Under s.12 of the CSIS Act, CSIS collects information in Canada and abroad and uses it as the basis for providing advice to the Government of Canada about activities that may constitute a threat to the security of Canada. This information is collected from many sources, including:

- members of the public;

- foreign governments;
- human sources;
- technical interception of telecommunications; and
- open sources including newspapers, periodicals, academic journals, foreign and domestic broadcasts, official documents, and other published material.

ODAC does not collect PI (it uses information already collected and residing in the corporate holdings of CSIS) and the collection processes, data sources and technology used outside of the ODAC environment are not in scope. Also, ODAC only looks at metadata – the specific content associated with the metadata (e.g., an email message or telephone conversation) is not accessed by ODAC and therefore out of scope.

Terminology

Definitions:

Access Request	A request for access to a record made under the <i>Access to Information Act</i> .
Administrative Purpose	The <i>Privacy Act</i> defines an "administrative purpose" to be the use of an individual's personal information in a decision making process that directly affects that individual.
Access to Information Act	Provides a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public that necessary exceptions to the right of access should be limited and specific, and that decisions on the disclosure of government information should be reviewed independently of government.
Annual Report	A report on a government institution's administration of the <i>Access to Information Act</i> or the <i>Privacy Act</i> during the fiscal year, which is prepared by the head of a government institution for submission to Parliament.
Applicant or Requester	A Canadian citizen, a permanent resident, or any individual or corporation present in Canada that requests access to a record under the <i>Access to Information Act</i> ; a Canadian citizen, a permanent resident, or any individual present in Canada who requests access to a record under the <i>Privacy Act</i> .
Complainant	A person who makes a complaint to the Information Commissioner on any of the grounds outlined in subsection 30(1) of the <i>Access to Information Act</i> or to the Privacy Commissioner on any of the grounds outlined in subsection 29(1) of the <i>Privacy Act</i> .
Confidentiality	The Government Security Policy (2002) defines "confidentiality" to be the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the <i>Access to Information Act</i> and the <i>Privacy Act</i> .
Consistent use	A use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect the information to be used for a consistent purpose, even if the use is not spelled out.
Coordinator (Access to Information or Privacy)	Officer designated in each government institution to coordinate all activities within the institution relating to the application of the <i>Access to Information Act</i> , <i>Access to Information Regulations</i> , and related policy, directives, and guidelines.
Court	Means the Federal Court of Canada.

SECRET

Delegate	Is an officer or employee of a government institution who has been delegated to exercise or perform the powers, duties, and functions of the head of the institution under the <i>Access to Information Act</i> or the <i>Privacy Act</i> .
-----------------	---

Excluded Information	Information to which the <i>Access to Information Act</i> or the <i>Privacy Act</i> does not apply.
Exempt Bank	A personal information bank (PIB) that describes files consisting primarily of personal information related to international affairs, defence, law enforcement, and investigation. The head of a government institution can refuse to disclose any personal information requested that is contained in an Exempt Bank.
Exemption	A mandatory or discretionary provision under the <i>Access to Information Act</i> or the <i>Privacy Act</i> that authorizes the head of a government institution to refuse the disclosure of records in response to an access or privacy request.

Head	Is the minister, in the case of a department or ministry of state. In any other case, it is the person designated by Order in Council and, if no such person is designated, it is the chief executive officer of the institution, whatever their title.
Info Source	A series of annual Treasury Board of Canada Secretariat publications in which government institutions describe their functions, programs, activities, and information holdings, including collections of personal information. The Info Source publications also provide summaries of court cases and statistics on access to information and privacy requests.
Institution-Specific Bank	A type of personal information bank (PIB) that describes personal information about members of the general public and federal employees (current and former) that is contained in the records of a specific federal government institution. This type of PIB is recognized by the unique identifier PPU or PPE.

Manuals	Manuals used by employees of a government.
Metadata	Structured information that describes the data; allowing management, control and understanding of other information.
Open Source	Produced from publicly available information that is collected, exploited, and analyzed in a timely manner to produce actionable intelligence.

Personal Information	Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing" that appears prior to the list of examples. Information that is not specifically mentioned in the list of examples may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank	A collection or grouping of personal information under the control of a government institution which has been used, is being used or is available for use for an administrative purpose, or is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. A description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol, or other particular assigned only to that person. The personal information described in the PIB has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The Office of the Privacy Commissioner of Canada describes "privacy" as meaning "...the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."
Privacy Act	Protects the privacy of individuals with respect to personal information about themselves held by a government institution and provides individuals with a right of access to that information.

Privacy Commissioner	Is an Officer of Parliament appointed by Governor in Council, whose main function is to investigate complaints made by individuals under the <i>Privacy Act</i> and the <i>Personal Information Protection and Electronic Documents Act</i> .
Record	Means any documentary material, regardless of medium or form.
Record Number	A unique identifying number created by each institution for each Class of Record description using the institution's Federal Identity Program acronym (or commonly used acronym) and the institution's reference number.
Requester or Applicant	A Canadian citizen, a permanent resident, or any individual or corporation present in Canada who requests access to a record under the <i>Access to Information Act</i> ; a Canadian citizen, a permanent resident, or any individual present in Canada who requests access to a record under the <i>Privacy Act</i> .
Retention and Disposal Standards	Identifies the length of time records are maintained under the control of an institution and the point at which the final disposition is applied.

Acronyms:

ADM	Assistant Deputy Minister
ATIP	Access to Information and Privacy
CSIS	Canadian Security Intelligence Service
GoC	Government of Canada
GSP	Government Security Policy
N/A	Not Applicable
N/D	Not Determined
ODAC	Operational Data Analysis Centre
OPC	Office of the Privacy Commissioner of Canada
PDPP	Treasury Board, Privacy and Data Protection Policy
PI	Personal Information

SECRET

PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PSC	Public Safety Canada
SIRC	Security Intelligence Review Committee
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment

Reference

CSIS Operational Policy
CSIS Act

Participants

The following participants contributed to the development of the PIA and its report:

Gordon Kirk

Legal Services

Consultations and briefings:

Lara McGuire Ives OPC
Lindsay Scotton OPC

Note: Most of the information reported here was derived from interviews with the participants listed.

2.0 Business Process and Data Flow Analysis

Introduction

The CSIS collects and analyzes information and security intelligence from across the country and abroad and reports to and advises the Government of Canada on national security issues and activities that threaten the security of Canada. The activities that constitute a threat to the security of Canada include:

- terrorism (serious violence for the purpose of achieving a political, religious or ideological objective);
- proliferation of weapons of mass destruction;
- espionage;
- transnational criminal activity; and
- foreign-influenced activity.

In planning and conducting an investigation, care is taken to ensure an appropriate balance between the degree of intrusiveness of an investigation and the rights and freedoms of those being investigated. Investigations that require use of more intrusive techniques, such as the interception of telecommunications, are subject to a rigorous process of challenge and controls, including the use of a Federal Court warrant.

Background

Understanding how the ODAC initiative developed requires recognizing the need for new architectures on which to build data exploitation capabilities that enhance the investigation of digital data.

The issues surrounding processing large quantities of digital data are well established.

The Service felt it critical to improve the capability to process data that contains context relevant information to present to an investigator. To this end, the concept of an ODAC introduces the notion of data exploitation

To derive more value from the data collected by the Service, ODAC was established with the vision of developing a data exploitation environment, recognized as a centre of excellence to more rigorously exploit and analyze the data collected to derive new information and combine that information to create knowledge to better achieve its mission.

SECRET

Again, the process of

defines data exploitation. ODAC, using advanced technology is creating a data exploitation environment 1

Governance Structure

The Deputy Director Operations, who reports to the Director of CSIS, is responsible for

ODAC is situated within

SECRET

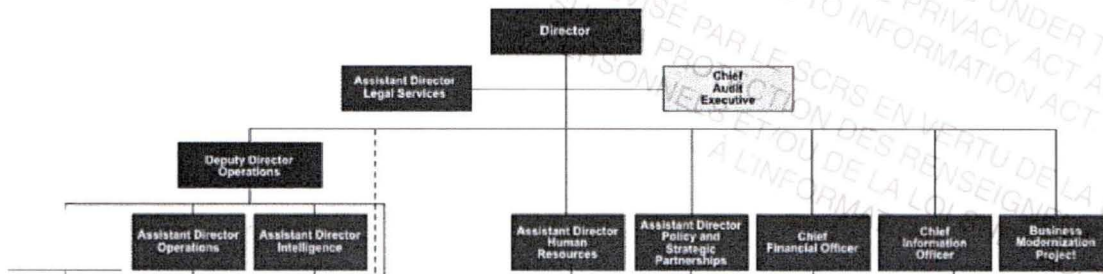


Figure 1 - Organization of CSIS

ODAC Concept

ODAC is a new and separate organizational services in support of operational programs. The ODAC will implement increasingly sophisticated analytical capacity by deploying specialized, advanced analytical tools against a variety of sources of data. committed to providing data exploitation

SECRET

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Collection of Personal Information

The Service uses a variety of collection methods to investigate individuals or groups whose activities are suspected of constituting a threat to national security. Through investigations, the Service can identify individuals with suspected connections to terrorism and persons operating in Canada on behalf of hostile intelligence services. Information from members of the public, foreign governments and technical interception of communications are combined with information from open sources including newspapers, periodicals, academic journals, foreign and domestic broadcasts, official documents and other published material.

ODAC does not collect any personal information; it accesses corporate information holdings (SIS PPU 015 and SIS PPU 045) duly authorized for collection in support of investigations.

Analysis

ODAC does not collect any personal information, but rather uses tools and rich data analysis techniques to assist its analysts.

Data Content

ODAC uses only metadata – data describing data – in its process. Metadata provides information about a data record that ODAC analysts exploit using information technology systems and applications, but it does not contain the actual business content.

SECRET

Dissemination of Information

The *CSIS Act* designates the Government of Canada as the main recipient of CSIS intelligence. Stated elsewhere in this report is an explanation of disclosure under section 19 of the *CSIS Act* however it is also important to acknowledge that ODAC does not disclose personal information; its analysts provide reports back to the lead regional/operational analyst that they are assisting. ODAC does not disclose information outside the Service.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Applicable Legislation, Regulation and Policy

This section lists relevant legislation and policies that have a potential bearing on privacy requirements of the N-III program, including any departmental program statutes and policies, namely:

Access to Information Act, R.S.C. 1985, c. A-1:

<http://laws.justice.gc.ca/en/A-1/index.html>

Access to Information Policy:

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_121/siglist_e.asp

Active Monitoring Policy:

http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/am-sa/am-sa_e.asp

Auditor General Act, R.S.C. 1985, c. A-17

<http://laws.justice.gc.ca/en/A-17/text.html>

Canadian Charter of Rights and Freedoms

<http://laws.justice.gc.ca/en/charter/index.html>

Canadian Security Intelligence Service Act

<http://www.canlii.org/ca/sta/c-23/>

Department of Public Works and Government Services Act:

<http://www.canlii.org/ca/sta/p-38.2/>

Electronic Authorization and Authentication, Policy on:

http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/TBM_142/2-2_e.asp

Government Records Disposition Program of the National Archives of Canada:

http://www.archives.ca/06/0611_e.html

Government Security Policy and Associated Policies and Publications:

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/siglist_e.asp

Integrated Risk Management Framework:

http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

Library and Archives of Canada Act, S.C. 2004, c. 11.

<http://laws.justice.gc.ca/en/L-7.7/index.html>

Management of Information Technology Policy:

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_IT/mit-gti_e.asp

Privacy Impact Assessment Policy:

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp

Privacy Act Regulations

<http://laws.justice.gc.ca/en/P-21/SOR-83-508/index.html>

Privacy Act, R.S.C. 1985, c. 1 (3rd Supp.):

<http://laws.justice.gc.ca/en/P-21/index.html>

Privacy and Data Protection Policy:

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/siglist_e.asp

Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks:

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1_e.asp

Public Key Infrastructure Management in the Government of Canada, Policy for:

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_e.asp

Security of Information Act:

SECRET

<http://www.canlii.org/ca/sta/o-5/>.

Technical Security Standard for Information Technology (TSSIT):

<http://jya.com/rcmp1.htm>.

Use of Electronic Networks, Policy on the:

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/tb_cp/uen2-2_e.asp.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

3.0 Privacy Analysis

The purpose of the privacy analysis is to examine the first phase of the ODAC initiative in the context of applicable privacy policies and legislation. Questionnaire "A" for Federal Programs and Services contained in the document entitled *"Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks"*, amended August 2, 2002 ("PIA Guidelines Questionnaires") was used as the basis for the privacy analysis. It is centered on the ten privacy principles of the *Model Code for the Protection of Personal Information* approved and published by the Canadian Standards Association (CSA) as a national standard in 1996 (CSAMC)².

These are the ten privacy principles:

Accountability	Accuracy
Identifying Purposes	Safeguards
Consent	Openness
Limiting Collection	Individual Access
Limiting Use, Disclosure and Retention	Challenging Compliance

A response of "N/D" (Not Determined) denotes that an answer to the questions is not possible. As ODAC is an evolving, phased development, it is necessary to assess these further and update the PIA reported here. A response of "N/A" (Not Applicable) indicates questions that are outside the scope of the PIA or otherwise do not apply.

The series of questions below are derived from the requirements of the *Privacy Act* and dovetail with universal privacy principles. Answers to the questions were developed within the context of the limited scope of the ODAC business process, the *CSIS Act* and CSIS' operational policy.

CSIS Operational Policy

CSIS administrative, security, human resources and operational policies embody rules and procedures that govern the range of activities undertaken by the Service. Operational policies, which describe how CSIS employees should perform their duties, are updated regularly in accordance with government policy, legislative and other changes. These operational policies shape the day-to-day activity of everyone working at and with CSIS. ODAC personnel follow operational policies and their associated procedures that pertain to, among others things, targeting levels and approvals process, as well as warrant powers and information management.

² The CSAMC Code forms Schedule 1 of PIPEDA and can be viewed at:
http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/sche1E.html

Privacy Act Principle 1: Accountability for Personal Information			
Questions For Analysis	Yes	No	N/D or N/A
<p>1.1 Has responsibility for the PIA been assigned?</p> <p>Please indicate in the details column the name and position of the person responsible.</p>	Yes		<p>The PIA is the joint responsibility of</p> <p>and the ATIP branches.</p> <p>The contacts are:</p> <p>Access to Information and Privacy Coordinator P.O. Box 9732 Station T Ottawa, Ontario, K1G 4G4</p> <p>ODAC P.O. Box 9732 Station T Ottawa, Ontario, K1G 4G4</p>
<p>1.2 Has the custody and control of personal information been determined?</p>	Yes		<p>ODAC holds this responsibility for ODAC derived information.</p>
<p>1.3 Has the accountability of the program custodian of personal information been documented?</p>		No	<p>Specific accountability for the handling of personal Information (PI) is not documented for ODAC.</p> <p>However, all employees play a role in supporting the in the effective management of all information in</p>

			<p>their custody. Departmental policies found in the <i>Operations Manual</i> (Appendix A) clearly state employees' security and information management (IM) responsibilities ensuring sound accountability for protecting and handling information – including PI.</p> <p>In addition the ATIP office provides awareness sessions and conducts oversight activities.</p>
1.4 Are the performance requirements of the custodian set out in a measurable way and subject to performance and compliance reviews?	No		<p>The Information Management (IM) group on behalf of directs and supports effective and efficient management of information through rigorous protocols to implement the Treasury Board (TB) <i>Policy on Information Management, Policy Framework for Information and Technology</i> and the supporting directives and standards.</p> <p>ODAC follows these protocols for data retention and disposal.</p>
1.5 Are third parties including the private sector involved in the custody or control of the personal information?	No		
1.6 If third parties or private sector parties are involved, do you have an agreement in place that establishes privacy requirements?	N/A		

1.7 If yes to 1.5, are the requirements of the <i>Personal Information Protection and Electronic Documents Act</i> applicable if the proposal involves the private sector?			N/A
1.8 Will the department be provided with the results of regularly scheduled audits and compliance checks on the privacy requirements of all involved parties?		Yes	Any audits/compliance checks conducted are available to involved parties.
1.9 Are the requirements for the Treasury Board <i>Policy on Privacy and Data Protection</i> being followed?	Yes		The Privacy Coordinator acts to ensure compliance with the <i>Privacy Act</i> , Regulations and associated policies.
1.10 Are there any requirements in program legislation or policies on the management of personal information that affect the proposal?	Yes		Section 18 of the <i>CSIS Act</i> constrain the use of intrusive information gathering techniques.

Discussion/Notes:

There are several accountability mechanisms designed to shape operational activities including those of ODAC. The Service remains accountable for its operations through the apparatus of government, specifically the Minister of Public Safety, the Inspector General of CSIS, the central agencies, the Auditor General, the Information Commissioner and the Privacy Commissioner of Canada. In addition the Security Intelligence Review Committee (SIRC) plays an accountability role.

A system of control and review mechanisms and processes, prescribed by the *CSIS Act*, include the following:

- Minister of Public Safety Canada: The Minister is responsible to Parliament for CSIS as a whole and for its general direction. The Minister issues the Ministerial Directive, policy guidelines concerning operational procedures, is informed of security operations and problems and approves cooperative agreements and relationships with foreign agencies.
- Deputy Minister of Public Safety Canada: The Deputy Minister provides advice to the Minister on general direction to CSIS and monitors how CSIS implements this direction.
- Director of CSIS: The Director of CSIS is accountable to the Minister for the management and control of CSIS. The Director submits periodic reports on CSIS activities to the Minister and chairs internal committees that are aimed at enhancing the organization's management and accountability. Two of these committees are directly responsible for, and have authority over, CSIS' use of investigative techniques. Under Section 20(2) of the *CSIS Act*, the Director of CSIS must submit a report to the Minister when, in the Director's opinion, a CSIS employee may have acted unlawfully in performing his or her duties or functions. The Minister, in turn, must send the report with his or her comments to the Attorney General of Canada and to SIRC.
 - CSIS Director's Annual Report: Yearly, the Director of CSIS submits a classified report to the Minister of Public Safety. It describes in detail the priorities and operational activities of the Service. The Inspector General of CSIS examines this report and

submits to the Minister a certificate that attests the extent satisfaction with its contents. Section 38(a) of the *CSIS Act* compels the Minister to send a copy of both documents to SIRC for its review.

- **Security Intelligence Review Committee (SIRC):** The SIRC is the body with a mandate to carry out ongoing, independent review of the activities of CSIS. Established under the *CSIS Act*, SIRC provides assurance to Parliament – and through it, to Canadians – that CSIS performs its duties and functions appropriately and effectively and in accordance with legislation, policy and Ministerial Direction. In doing so, SIRC seeks to ensure that CSIS both protects and respects the fundamental rights and freedoms of Canadians. SIRC is responsible for reviewing how CSIS performs its functions and investigates complaints against CSIS. The Committee also investigates complaints filed by individuals who were denied security clearances and reviews reports concerning immigration applications and citizenship applications that were rejected based on security or criminal grounds. To enable it to fulfill its responsibilities, the Committee has access to all information under CSIS' control (except Cabinet confidences). SIRC informs the Minister of Public Safety of its investigation findings on an ongoing basis, and produces an annual report that is tabled by the Minister in Parliament.
 - To fulfill its mandate, SIRC directs staff to undertake a number of reviews each year. These provide a retrospective examination and assessment of specific CSIS investigations and functions. Under the *CSIS Act*, SIRC has virtually unlimited power to review CSIS's performance. With the sole exception of Cabinet confidences, SIRC has the right to have access to any information under the control of the Service, no matter how highly classified that information may be.
 - SIRC's reviews include findings and, where applicable, recommendations. Upon completion, the report is forwarded to both the Director of CSIS and the Inspector General of CSIS. SIRC is also authorized under Section 54 of the *CSIS Act* to provide special reports to the Minister of Public Safety on any matter that the Committee identifies as having special importance or that the Minister directs SIRC to undertake.
- **Inspector General:** The Inspector General is responsible for monitoring CSIS' compliance with operational policies, reviewing its operational activities and reviewing and issuing a certificate indicating the degree of satisfaction with the Director's annual operational report. The certificate and the report are forwarded to the Security Intelligence Review Committee (SIRC). At the request of the Minister or SIRC, the Inspector General may conduct a review of specific CSIS activities. The Inspector General has access to all information under CSIS' control (except for Cabinet confidences). Every year, the Inspector General submits a certificate to the Minister stating the extent to which he or she is satisfied with the CSIS Director's Annual Report. This certificate informs the Minister of any unreasonable or unnecessary exercise of CSIS powers, as well as any instances of the Service failing to comply with either the *CSIS Act* or Ministerial Direction.
 - In the most recent certificates, the Inspector General was satisfied with the CSIS Director's Annual Reports, stating that the Service has not acted beyond the framework of its statutory authority, had not contravened any Ministerial Directions and had not exercised its powers unreasonably or unnecessarily.
- **Federal Court:** The power to authorize intrusive investigation techniques rests solely with the Federal Court of Canada. Before such an authorization can be made, CSIS must provide solid justification for the proposed use of these techniques in an affidavit, which is reviewed by a senior CSIS committee chaired by the Director and comprised of representatives from the Department of Justice and Public Safety Canada. If the committee endorses the intrusive technique, the affidavit is submitted to the Minister of Public Safety Canada for approval. If the Minister gives approval, the affidavit is then submitted to the Federal Court, which must issue a warrant before CSIS can proceed with the intrusive investigative technique.
- **Public Reporting:** CSIS provides information to Parliament and the public through the Minister's Annual Statement on National Security and the CSIS Public Report. These

documents provide Canadians with an assessment of the current security intelligence environment and detail the government's efforts to ensure national security. More specifically, the CSIS Public Report is aimed at increasing awareness of CSIS' functions and the processes it employs, and dispelling some of the myths surrounding security intelligence work.

- **Access to Information and Privacy (ATIP):** The Access to Information and Privacy (ATIP) Section is located within the Secretariat Branch of the Assistant Director Policy and Strategic Partnership (ADP) and works to fulfill the Service's obligations under the *Access to Information and Privacy Acts*. The CSIS Legal Services Branch provides legal advice as required. The mandate of the ATIP Section is to act on behalf of the Minister of Public Safety Canada in promoting and enforcing compliance with legislation, regulations and government policy and to create departmental directions, including standards, in all matters relating to the *Access to Information Act* and *Privacy Act* within CSIS. The Coordinator also acts as spokesperson for the organization in dealing with the Treasury Board Secretariat, the Information and Privacy Commissioners and other government departments and agencies.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Privacy Act Principle 2: Collection of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
<p>2.1 What is your authority to collect personal information?</p> <p>Please indicate the authority. If there is no authority, please consult with your legal advisor to determine if there is authority to proceed.</p>				<p>Section 12 and Section 21 of the CSIS Act. ODAC does not collect any information but uses PI already collected as authorized by the warrant application and approval process.</p>
<p>2.2 Is the personal information collected directly related to an operating program or activity? s. 4</p>	Yes			<p>See 2.1</p> <p>ODAC directly supports only authorized activities and investigations approved before ODAC becomes involved.</p>
<p>2.3 Is personal information being collected directly from the individual? s. 5(1)</p> <p>If no, why not?</p>		No		<p>The activities the Service engages in are not conducive to collecting information directly from the individual for reasons of national security investigations.</p> <p>Collecting information directly from individuals would jeopardize the ability to conduct investigations and carry out the CSIS mandate.</p> <p>ODAC does not collect any personal information.</p> <p>See 2.1</p>
<p>2.4 Have the purposes for which the personal information is collected been documented?</p> <p>If yes, provide specifics. s. 4</p>	Yes			<p>Although ODAC does not collect information, the information it uses was collected and documented as defined in the CSIS Act.</p>
<p>2.5 Is all the personal information collected necessary to the operating program or activity?</p>	Yes			
<p>2.6 Is there notice at the collection stage that</p>		No		See 2.3

identifies the specific purposes for the collection, the authority for doing so and the individual serving as official contact? s. 5(2)			
2.7 Is the notice associated with the collection of personal information available and consistent across all mediums of collection? s. 5(2)		N/A	See 2.3
2.8 Are secondary uses contemplated for the information collected? s. 7 If yes, describe them in the details column.	No		
2.9 If personal information is to be used or disclosed for a secondary purpose not previously identified, is consent required? s. 7 & 8		N/A	
2.10 If consent is not required for secondary purpose use or disclosure, is there authority for the use or disclosure? s. 7 & 8		N/A	
2.11 Is information anonymized when used for planning, forecasting and/or evaluation purposes?	Yes		
2.12 Is personal information collected from a public database?	Yes		ODAC does not collect PI but the data it uses is metadata from many sources
2.13 Will quality assurance or security activities result in the collection of additional personal information?	No		
2.14 Does the program or activity involve the collection through a common client identifier? If yes, provide details about the identifier.	Yes		ODAC may use _____ to search for data that is relevant. Search parameters are developed

A. ODAC does not collect any PI but it uses the PI already collected by the Service. This PIA is only focused on ODAC, therefore a detailed assessment of the Service's collection activities is out of scope, however following is a general discussion outlining the authority of the Service, mandated under the *CSIS Act* to collect PI that may help reviewers.

- The Act strictly limits the type of activity that may be investigated, the ways that information can be collected and who may view the information. Information may be gathered primarily under the authority of section 12 of the Act and must pertain to those individuals or organizations suspected of engaging in activities that may threaten the security of Canada (i.e., espionage, sabotage, political violence, terrorism and clandestine activities by foreign governments).
- The *CSIS Act* prohibits the Service from investigating acts of lawful advocacy, protest or dissent. CSIS may only investigate these types of acts if they are linked to threats to Canada's national security.
- Sections 14 and 15 authorize CSIS to conduct security assessments used during the visa application process and the application process for refugees and Canadian citizenship.

- The *Immigration and Refugee Protection Act* provides for security screening of people in the refugee stream who may pose security risks and allows for their early removal from Canada. This legislation strengthens Canada's ability to detect and refuse entry to suspected terrorists.
- The *Anti-terrorism Act* creates measures to identify, deter, disable and prosecute those engaged in terrorist activities or those who support these activities. The legislation makes it an offence to knowingly support terrorist organizations, whether through overt violence, or through material support. The *Anti-terrorism Act* requires the publication of a list of groups deemed to constitute a threat to the security of Canada and to Canadians.
- The *Security of Information Act* legislates various aspects of security of information, including the communication of information, forgery, falsification of reports, unauthorized use of uniforms and entering a prohibited place.
- The *Public Safety Act* enhances the ability of the Government of Canada to provide a secure environment for air travel and allows specified federal departments and agencies to collect passenger information for the purpose of national security. It also establishes tighter controls over explosives and hazardous substances and deters the proliferation of biological weapons. While the *Anti-Terrorism Act* focuses mainly on the criminal law aspects of combating terrorism, this legislation addresses the federal framework for public safety and protection.

Canadian Security Intelligence Service 31
Operational Data Analysis Centre
Privacy Impact Assessment

are verified during the preparation stage and reviewed again by an "independent counsel" from the Department of Justice to ensure that the affidavits are legally and factually correct prior to their submission to the Federal Court which must issue a warrant before CSIS can proceed with the intrusive investigative technique for collecting PI.

B. The CSIS Act clearly defines the process and requirements for obtaining a warrant and constrains investigative techniques and the PI collected in accordance with the warrant issued. Although this is done before ODAC becomes involved, the following is an excerpt from the Act to help illustrate how the warrant process works:

The Warrant Process

Application for a warrant:

21. (1) Where the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the approval of the Minister, make an application in accordance with subsection (2) to a judge for a warrant under this section.

(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by an affidavit of the applicant deposing to the following matters, namely,

- (a) the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16;
- (b) that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (a) would not be obtained;
- (c) the type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained and the powers referred to in paragraphs (3)(a) to (c) proposed to be exercised for that purpose;
- (d) the identity of the person, if known, whose communication is proposed to be intercepted or who has possession of the information, record, document or thing proposed to be obtained;
- (e) the persons or classes of persons to whom the warrant is proposed to be directed;
- (f) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;
- (g) the period, not exceeding sixty days or one year, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (5); and
- (h) any previous application made in relation to a person identified in the affidavit pursuant to paragraph (d), the date on which the application was made, the name of

the judge to whom each application was made and the decision of the judge thereon.

Issuance of Warrant

(3) Notwithstanding any other law but subject to the *Statistics Act*, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(a) and (b) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,

- (a) to enter any place or open or obtain access to any thing;
- (b) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or
- (c) to install, maintain or remove any thing.

Matters to be specified in warrant

(4) There shall be specified in a warrant issued under subsection (3)

- (a) the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained and the powers referred to in paragraphs (3)(a) to (c) authorized to be exercised for that purpose;
- (b) the identity of the person, if known, whose communication is to be intercepted or who has possession of the information, record, document or thing to be obtained;
- (c) the persons or classes of persons to whom the warrant is directed;
- (d) a general description of the place where the warrant may be executed, if a general description of that place can be given;
- (e) the period for which the warrant is in force; and
- (f) such terms and conditions as the judge considers advisable in the public interest.

Maximum duration of Warrant

(5) A warrant shall not be issued under subsection (3) for a period exceeding

- (a) sixty days where the warrant is issued to enable the Service to investigate a threat to the security of Canada within the meaning of paragraph (d) of the definition of that expression in section 2; or
- (b) one year in any other case.

Privacy Act Principle 3: Consent

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
3.1 Is consent obtained directly from the individual? If not, why not?		No		See 2.3
3.2 How is consent obtained?			N/A	
3.3 Does consent require a positive action by an individual rather than being assumed as a default? s. 5, 7 & 8			N/A	
3.4 If yes to 3.1 is the consent clear and unambiguous?			N/A	
3.5 If consent is sought, is the form of consent likely to stimulate negative reaction (for example, opt-in or -out)?			N/A	
3.6 Can an individual refuse to consent to the collection or use of personal information for a secondary purpose, unless required by law?			N/A	
3.7 Would the refusal of an individual to consent to the collection or use of personal information for a secondary purpose disrupt the level of program service provided to the individual?			N/A	
3.8 Are standards and mechanisms in place to ensure that the individual has capacity to give consent? s. 77(1)(m)			N/A	
3.9 Are standards and mechanisms in place to ensure the recognition of persons authorized to make decisions on behalf of others (e.g. a minor or incapacitated person)? If not why not? s. 77(1)(m)			N/A	

SECRET

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Privacy Act Principle 4: Use of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
<p>4.1 What is your authority to use personal information? Please indicate the authority.</p> <p>If there is no authority please consult your legal advisor to determine the authority to proceed with the proposal.</p>				<p>The CSIS Act.</p> <p>See 2.1 and the associated discussion notes.</p>
4.2 Is personal information used exclusively for the purpose for which the information was obtained or compiled? s. 7 (a)	Yes			
4.3 Are the uses of the information limited to what a reasonable person would consider appropriate in the circumstances?	Yes			
4.4 Is personal information used for a purpose for which the information may be disclosed to the program by another institution? s. 7 (b)	Yes			
4.5 Are personal identifiers, such as a social insurance number, used for the purposes of linking across multiple databases?	Yes			<p>CSIS does not use SIN numbers. Specific</p> <p>are used.</p>
4.6	Yes			
4.7		No		

4.8			N/D	
4.9 Is there an activity log attached to the personal information record to record uses not in the Index of Personal Information Banks? s. 9(1)?			N/D	PI is used in accordance with the Index of PIBS.
4.10 Is personal information used for a consistent purpose that is not identified in a personal information bank? s.9(4)		No		PI is used for a consistent purpose identified in the PIB.

Discussion/Notes:

A. Following are details of the PIB SIS PPU 045, Canadian Security Intelligence Service Investigational Records that applies to ODAC activities.

Description: The records described in this bank include personal information on identifiable individuals whose activities are suspected of constituting threats to the security of Canada; on identifiable individuals who are or were being managed as confidential sources of information; on identifiable individuals no longer investigated by CSIS but whose activities did constitute threats to the security of Canada and which still meet the collection criteria stipulated in section 12 of the *CSIS Act*, and on identifiable individuals the investigation of whom relate to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities. Exempt Bank Status: This bank has been designated as an exempt bank by Order-in-Council No. 14 (CSIS) dated 26 November 1992.

Class of Individuals: Individuals suspected of espionage or sabotage against Canada or the interests of Canada; individuals involved in foreign influenced activities within or relating to Canada that are clandestine or deceptive or involve a threat to any person; individuals involved in activities within or related to Canada directed toward the use of serious acts of violence to achieve a political, religious or ideological objective within Canada or a foreign state; or individuals whose activities are directed toward the unlawful covert undermining, or the overthrow by violence, of the constitutionally established government system in Canada; or any other activities described in the definition of "threats to the security of Canada" at section 2 of the *CSIS Act*; individuals identified relating to a national security concern, the defence of Canada or the conduct of the international affairs of Canada; and individuals who are confidential sources of information.

Purpose: Collected under section 12 of the *CSIS Act* with respect to threats to the security of Canada; under section 15 concerning the collection of information for the purpose of providing advice pursuant to section 14; and under section 16 concerning the collection of information or intelligence relating to the capabilities, intentions or activities of foreign states and certain persons.

Consistent Uses: CSIS may only disclose information it obtains if it does so in accordance with the controls of subsection 19(2) of the *CSIS Act*. First, it may disclose information for the purposes of the performance of its duties and functions under the *CSIS Act* or the administration or enforcement of

SECRET

that Act, or as required by any other law. The Service may thus disclose personal information to the Government of Canada, for example, as part of its duty to report and give advice thereto in relation to activities suspected of constituting threats to the security of Canada. Secondly, where the information in its possession may be used in the investigation or prosecution of an alleged contravention of the law, or where it relates to the conduct of Canada's international affairs or to the defence of Canada, then it may be disclosed to the appropriate police officials and to the Attorney General, to the Minister of Foreign Affairs and to the Minister of National Defence, respectively. Thirdly, information may be disclosed where, in the opinion of the Minister, disclosure to any Minister of the Crown or person in the Public Service of Canada is essential in the public interest and that interest clearly outweighs any invasion of privacy that could result from the disclosure. Pursuant to section 13 and 14 of the *CSIS Act*, CSIS may also disclose information in the preparation of a domestic or foreign security assessment, or in providing advice under the *Citizenship Act* or *Immigration and Refugee Protection Act*. Personal information may also be disclosed to the Inspector General and the Security Intelligence Review Committee. Information in this bank may also be used for audit, research, planning, evaluation and statistical purposes.

Retention and Disposal Standards: Information in this bank is retained for at least twenty years after the last action, subject to the retention and disposal standards of CSIS. When files have been designated as historical, they may be transferred to the custody and control of Library and Archives Canada and where the record has not been so designated, it shall be destroyed.

RDA Number: 2006/001

Related Record Number: SIS DDS 010

TBS Registration: 002872

Bank Number: SIS PPU 045

Privacy Act Principle 5: Disclosure and Disposition of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
5.1 Is personal information disclosed with the consent of the individual? S. 8(1)		No		ODAC does not disclose information outside of CSIS.
5.2 If personal information is not disclosed with consent, has the specific authority for disclosure been identified? s. 8(2) If there is no authority to disclose personal information, please consult your departmental legal advisor.	Yes			Section 8 (2)(b) of the Privacy Act.
5.3 Are personal identifiers, such as a social insurance number, disclosed?			N/A	
5.4 Is the personal information to be disclosed limited to the purpose of disclosure?			N/A	
5.5 Is personal information disclosed for a purpose that is not identified			N/A	

in a personal information bank? s. 9(4)			
If yes, what is the method planned for disposal?			
5.6 Will personal information be processed, disclosed or retained outside of Canada?	No		
5.7 Is there an activity log attached to the personal information record to record the purposes of disclosure not listed in the Index of Personal Information Banks? s. 9(1)?		N/A	
5.8 Is the personal information scheduled for retention and disposition? s. 6(1) & (3)	Yes		Information in bank SIS PPU 045 is retained for at least twenty years after the last action, subject to the retention and disposal standards of CSIS.
If yes, identify where in details column.			
5.9		N/D	

Discussion/Notes:

A. ODAC does not disclose information outside the Service.

See section 2.0 for a description of the ODAC business process.

B. Disclosure of Information – General

Section 19 of the *CSIS Act* prohibits the disclosure of information obtained by the Service in the course of its investigations except in the following specific circumstances:

- Information that may be used in the investigation or prosecution of an alleged contravention of any federal or provincial law may be disclosed to a law enforcement agency having jurisdiction over the matter, or to the Minister of Public Safety or the Attorney General of the province in question;
- Information related to the conduct of Canada's external relations may be disclosed to the

SECRET

Minister of Foreign Affairs;

- Information related to the defence of Canada may be disclosed to the Minister of National Defence; and
- Information that, in the opinion of the Minister, is essential to the public interest, may be disclosed to any Minister of the Crown or employee of the Public Service of Canada.

Of note, Section 19(2)(d) of the *CSIS Act* gives the Minister of Public Safety the power to override any invasion-of-privacy concerns, authorizing the Service to disclose information deemed to be in the national or public interest. When such information is released, the Director of CSIS must submit a report to SIRC. This is an exceedingly rare occurrence.

C. Reportable Disclosures of Personal Information Under Section 8 of the Act

As a rule, the Service does not make any disclosures under the authorities provided by paragraphs 8(2)(e), 8(2)(f) and 8(2)(m) of the *Privacy Act*. The disclosure of personal information obtained in the performance of the duties and functions of the Service is made under subsection 19(2) of the *CSIS Act*, as authorized by paragraph 8(2)(b) of the *Privacy Act*.

Privacy Act Principle 6: Accuracy of Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
6.1 Will steps be taken to ensure that the personal information is accurate, complete and up-to-date? s. 6(2)	Yes			See section 2.0 for a description of the ODAC business process that shows the decision points that assess the pertinence and context of PI.
6.2 Does the record of personal information indicate the date of last information update?		No		See Discussion/Notes
6.3 Is a record kept of the source of the information used to make changes?	Yes			
6.4 Where applicable, is there a procedure, automatically or at the request of an individual, to provide notices of correction to third parties to whom personal information has been previously disclosed? S. 12(2)(c)	Yes			Section 41 of the CSIS Act provides a process.
6.5 Is there a record kept with respect of requests for a review of errors or omissions & corrections or decisions not to correct? s. 12(2)(b)	Yes			ATIP has a formal record keeping process (SIS PRN 930).
6.6 Is there a clearly defined process by which an individual may access, assess and discuss or dispute the accuracy of the record? Please briefly describe the steps?	Yes			Section 41 of the CSIS Act provides A process.

Discussion/Notes:

A. A clearly defined process exists for an individual to follow to make a complaint about any activity of the Service. Section 41 of the CSIS Act will apply and the process is published on the Service' website and InfoSource listing. It advises if an individual wishes to complain about CSIS activities under Section 41 of the CSIS Act, they must first file a complaint by writing to the Director of the Service and gives the address.

Anyone not satisfied with the Director's response, or if a response is not received within a reasonable

SECRET

time (usually 30 days), they may then submit a complaint to SIRC, including the response, if any, received from the Director of CSIS. The address for SIRC is listed and individuals are informed that once a complaint is received, SIRC will contact them to follow up on the information provided.

B. Integrity or quality means data cannot be created, changed or deleted without proper authorization. It also means that data stored in one part of a database or system is in agreement with other related data stored in another part of the database or system (or another system).

For example: A loss of integrity occurs when an employee accidentally, or with malicious intent, deletes important data files. A loss of integrity can occur when data is changed in one database but not in a related one. ODAC accesses a copy of data from data may have integrity problems if it is a copy. - that

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Privacy Act Principle 7: Safeguarding Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
7.1 Has a Threat and Risk Assessment been completed?		No		A TRA has not been completed.
7.2 Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented?	Yes			See discussion.
7.3 Are program and information technology staff trained in the requirements for protecting personal information and are they aware of the relevant policies regarding breaches of security or confidentiality?	Yes			See discussion.
7.4 Are there controls in place for any process to grant authorization to modify (add, change or delete) personal information from records?	Yes			See discussion.
7.5 Is the system designed so that access and changes to personal information can be audited by date and user identification?	Yes			See discussion.
7.6 Are user accounts, access rights and security authorizations controlled by a system or record management process?	Yes			See discussion.
7.7 Are access rights only provided to users on a "need to know basis" consistent with the stated purposes for which the personal information was collected? s. 5(2)	Yes			See discussion.
7.8 Are security measures commensurate with the sensitivity of the information recorded?	Yes			See discussion.
7.9 Are there contingency plans and documented procedures in place to identify and respond to security breaches or disclosures of personal information in error?	Yes			See discussion.

7.10 Are there documented procedures in place to communicate security violations to the data subject, law enforcement authorities and relevant program managers?	Yes	See discussion.
7.11 Is there a plan for quality assurance and audit programs to assess the ongoing state of the safeguards applicable to the system?	Yes	See discussion.

Discussion/Notes:

A. The ATIP and Internal Security Sections conduct ATIP and Security awareness sessions for all new CSIS employees. A number of briefing sessions were also given to managers and other specialized groups. The purpose of the sessions was to provide participants with an overview of the *Access to Information and Privacy Acts*, along with a better understanding of their obligations and the process within CSIS.

B. The Government Security Policy (GSP) and its associated operational standards and technical documentation prescribes the safeguards and how to deploy them to protect employees, preserve the confidentiality, integrity, availability and value of assets and assure the continued delivery of services. Although the GSP sets baseline security requirements – mandatory provisions – they are a minimum. CSIS defined and implemented security policies and operational standards that exceed the minimum prescribed by the GSP.

Also noteworthy, CSIS has government-wide responsibilities under the GSP to:

- Investigate and analyze physical and cyber threats to national security, as defined in the *CSIS Act*, and provide related advice. These threats include espionage and sabotage, foreign influence activity and politically motivated violence.
- Provide security and intelligence advice, including threat and risk assessment information, to departments.
- Conduct investigations and provide security assessments, as requested by departments for the processing of security clearances.
- Maintain a central index of security assessments conducted and resulting recommendations.

C. Following are security architecture Details:

SECRET

D. Clearly, CSIS is a highly secure organization that takes proactive steps that see it regularly exceed the GSP standard

This is the environment that ODAC operates within and what drives how it safeguards information.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Privacy Act Principle 8: Openness

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
8.1 Describe how the results of any privacy impact assessment or audit will be made available to the public.			N/A	Due to the extremely sensitive nature of the Service's activities in general and the highly sensitive investigative techniques/data sources used by ODAC the PIA will not be available to the public.
8.2 Are policies and practices relating to the proposal's management and handling of personal information available to the public?		No		See 8.1
8.3 Is there a communications plan to explain to the public how personal information will be managed and protected?		No		See 8.1
8.4 Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	Yes			Section 41 of the CSIS Act provides a process.
8.5 Where appropriate, have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the proposal?	Yes			Key stakeholders were involved in the PIA process.
8.6 Where appropriate, will public consultation take place on the privacy implications of the proposal?		No		See 8.1
8.7 Has the personal information been included in a personal information bank? s. 10	Yes			SIS PPU 015 (CSIS Records) and SIS PPU 045 (CSIS investigational

			Records, Exempt Bank).
--	--	--	---------------------------

Discussion/Notes:

Although CSIS will not share any information from the ODAC PIA process the following is offered to help reviewers understand CSIS' commitment to openness and sharing information with the public. CSIS stays in contact with the public through various programs and activities: Liaison/Awareness Program; Public Liaison and Outreach Program; Media Relations Program; Cross-cultural Roundtable on Security.

- The Liaison/Awareness Program provides for ongoing dialogue with private and public organizations on the threat posed to Canadian interests by foreign governments which engage in economic espionage. The program allows CSIS to collect and assess the information needed to investigate activities of economic espionage against Canada, while enabling Canadian companies and public organizations to reduce their vulnerability by more effectively protecting themselves.
- The Public Liaison and Outreach Program is aimed at informing the public about the role and activities of CSIS in supporting national security. In this context, the Public Liaison and Outreach officer responds to enquiries from the public, and, in cooperation with regional officers, identifies opportunities to raise public awareness about issues relating to CSIS.
- The Media Relations Program plays an important role in ensuring that media receives timely, accurate, balanced and consistent information from CSIS.
- A key element of the government's National Security Policy is the Cross-cultural Roundtable on Security, a forum aimed at engaging Canadians in a long-term dialogue on national security matters, recognizing that Canada is a diverse and pluralistic society. The Roundtable provides a forum to discuss emerging trends and developments stemming from national security matters and serves to inform policy-makers.

Privacy Act Principle 9: Individual's Access to Personal Information

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
9.1 Is the system designed to ensure that an individual can have access to his/her personal information including all other programs or applications that have received copies of the information? s. 12(10)		No		The activities the Service engages in are not conducive to providing individuals access to their PI for reasons of national security. Doing so would jeopardize the ability to conduct investigations and carry out the CSIS mandate.
9.2 Is the system designed to ensure that an individual has been notified that a correction to his/her information has been made?		No		See 9.1
9.3 Are all custodians and participants aware of an individual's right of access and the complaint process?	Yes			
9.4 Are there documented procedures developed or planned on how to initiate privacy requests or requests for the correction of personal information? s. 12(2)	Yes			Section 41 of the <i>CSIS Act</i> provides a process.
9.5 Has consideration been given to providing individuals "routine" access to their personal information?		No		See 9.1
9.6 Are individuals provided with access to their personal information in the official language of choice? s. 17(2)			N/A	Section 41 of the <i>CSIS Act</i> provides a process.

SECRET

9.7 If appropriate, are individuals provided with access to their personal information in alternative format? s. 17(3)

N/A Section 41 of the CSIS Act provides a process.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

Privacy Act Principle 10: Challenging Compliance

Questions For Analysis	Yes	No	N/D or N/A	Provide Details
10.1 Are the complaint procedures for the proposed program or service consistent with legislated requirements? s. 29-35	Yes			Section 41 of the CSIS Act provides a process.
10.2 To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	Yes			Section 41 of the CSIS Act provides a process.
10.3 Are there oversight and review mechanisms implemented or available to ensure accountability?	Yes			
10.4 Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal? If yes, please provide a summary of the above in the details column and append to final report.			N/D	See the discussion under privacy principle 1 – Accountability.

4.0 Privacy Risk Management Plan

This section summarizes the specific privacy risks identified through the PIA process related to ODAC and lists mechanisms to mitigate these risks anticipated to arise from the new functionality and use of data exploitation capabilities by CSIS creating an ODAC. **Although mitigation strategies are discussed, they are alternatives and implementation of all strategies is not necessarily required or appropriate to address specific privacy risks.** The nature and extent of any residual risks following implementation of mitigation strategies cannot be determined at this stage, as it is unknown how and to what extent mitigating mechanisms may be employed. It is recommended that residual risks be assessed following implementation of further phases.

Accountability

Risks	Risk Level	Risk Mitigation Measures
<i>There are no privacy risks identified.</i>	<i>N/A</i>	<i>N/A</i>

Collection of Personal Information

Risks	Risk Level	Risk Mitigation Measures
<i>There are no privacy risks identified.</i>	<i>N/A</i>	<i>N/A</i>

Consent

Risks	Risk Level	Risk Mitigation Measures
<i>There are no privacy risks identified.</i>	<i>N/A</i>	<i>N/A</i>

Use of Personal Information

Risks	Risk Level	Risk Mitigation Measures
<i>ODAC complies with Service's established policies and procedures.</i>	<i>Low</i>	Responsibility: <i>Ensure that Service's established policies and procedures are met.</i>

Disclosure and Disposition of Personal Information

Risks	Risk Level	Risk Mitigation Measures
<i>Disclosure and disposition of personal information is managed in accordance with the CSIS standards for retention and disposition.</i>	<i>Low</i>	Responsibility: <i>Continue to ensure that ODAC complies with the standards already established for information retention and disposal schedules established under the Government Records Disposition Program of the National Archives of Canada.</i>

Accuracy of Personal Information

Risks	Risk Level	Risk Mitigation Measures
	Low	<p>Responsibility:</p> <p>Recommendation:</p> <p>Develop processes to ensure that the data stored in the ODAC environment remains in agreement with to assure data integrity as it relates to authenticity, accuracy, currency and completeness.</p>

Safeguarding of Personal Information

Risks	Risk Level	Risk Mitigation Measures
ODAC is pioneering a new way of CSIS doing analysis – processes, data sources, IT tools.	Low	<p>Responsibility:</p> <p>Recommendation:</p> <p>Conduct a harmonized TRA project to ascertain the risk environment with an examination of information and their values, as well as threats and vulnerabilities to determine the acceptability of residual risks and if necessary, identify mitigation strategies and security safeguards.</p>
ODAC analysts embrace the need to share concept when conducting authorized investigations.	Low	<p>Responsibility:</p> <p>Recommendation:</p> <p>Ensure IT systems are safeguarded</p> <p>Develop a plan to ensure that access controls are put in place</p> <p>Recommendation:</p> <p>Develop a security audit regime</p>

Risks	Risk Level	Risk Mitigation Measures

Openness

Risks	Risk Level	Risk Mitigation Measures
<i>There are no privacy risks identified.</i>	<i>N/A</i>	<i>N/A</i>

Individual's Access to Personal Information

Risks	Risk Level	Risk Mitigation Measures
<i>There are no privacy risks identified.</i>	<i>N/A</i>	<i>N/A</i>

Challenging Compliance

Risks	Risk Level	Risk Mitigation Measures
<i>There are no privacy risks identified.</i>	<i>N/A</i>	<i>N/A</i>

5.0 Communications

CSIS believes in the principles of openness and transparency but must ensure that the information it shares with the public doesn't detract from its ability to protect Canadian citizens and interests from threats to national security. Due to the extreme sensitivity of the work that ODAC undertakes it is not possible to communicate about that work to the public – there will not be any public liaison or communication specifically about the activities ODAC undertakes because CSIS cannot disclose its operational methodologies.

However, CSIS does stay in contact with the public to keep it informed through various programs and measures:

- The Liaison/Awareness Program provides for ongoing dialogue with private and public organizations on the threat posed to Canadian interests by foreign governments that engage in economic espionage. The program allows CSIS to collect and assess the information needed to investigate activities of economic espionage against Canada, while enabling Canadian companies and public organizations to reduce their vulnerability by more effectively protecting themselves.
- The Public Liaison and Outreach Program aims to inform the public about the role and activities of CSIS in supporting national security. In this context, the Public Liaison and Outreach officer responds to enquiries from the public, and, in cooperation with regional officers, identifies opportunities to raise public awareness about issues relating to CSIS.
- The Media Relations Program plays an important role in ensuring that media receives timely, accurate, balanced and consistent information from CSIS.
- The Cross-cultural Roundtable on Security is key element of the government's National Security Policy providing a forum aimed at engaging Canadians in a long-term dialogue on national security matters, recognizing that Canada is a diverse and pluralistic society.

6.0 Conclusion

This PIA report, produced following the Treasury Board guidelines, describes the privacy-related impacts of the capacity building phase of ODAC and proposes mitigation strategies for the identified privacy risks associated with it. The assessment process has identified **no high privacy risks**. The privacy-related risks highlighted in this report are of lesser magnitude (six low risk items). Those risks concern the use of personal information; accuracy of personal information; disposition and retention requirements; and safeguarding personal information.

This report reflects the business model for ODAC as of the date of the report – it is a snapshot in time and scope. Because the design of the ODAC solution continues to evolve and will never be complete, it is necessary to ensure that the PIA process continues iteratively so that any new privacy issues are appropriately identified, analyzed and resolved – the Service will refresh the PIA process and update this report periodically so that it reflects the evolving data exploitation capabilities of ODAC.

As the ODAC project moves forward with implementing follow-on phases, privacy principles and fair information practices as outlined in both the *Standards Council of Canada's Model Code for the Protection of Personal Information* and the *Privacy Act* should continue to be designed into core program and project objectives. Appropriate development of the privacy risk management plan detailed herein must continue, with short-term focus upon addressing

Appendix A

OPS-601 AUTHORIZED DISCLOSURE OF OPERATIONAL INFORMATION AND INTELLIGENCE - GENERAL

1. INTRODUCTION

Objective

1.1 The primary mandate of the Service is to report to and advise the Government regarding threats to the security of Canada. This entails the disclosure of information and intelligence by the Service to various recipients in order to fulfil its duties and functions.

1.2 The flow of information or intelligence must be controlled to protect the rights of individuals and protect the security of the Service's operations therefore disclosures are made in compliance with the *CSIS Act*, Ministerial Direction, the Government Security Policy (GSP) and other relevant legislation.

Scope

1.3 This policy prescribes the general policy and guidelines for the disclosure of operational information and intelligence and of incidental information collected by the Service in compliance with the *CSIS Act*.

1.4 Subsequent chapters of this policy will detail the specific policy and procedures to be followed when disclosing information and intelligence to the different clients of the Service.

1.5 The particular procedures for the disclosure, recording and tracking of information or intelligence collected pursuant to s. 16 of the *CSIS Act* are contained in OPS-222, "HUMINT Collection - Section 16".

Authorities and References

1.6 *CSIS Act*

1.7 Ministerial Direction on CSIS Operations (2001 03 01)

1.8 Memorandum of Understanding between CSIS and the RCMP

1.9 Privy Council Office Directive of October 14 1986 on the Reporting of Security Investigations on Holders of Public Office

1.10 CSIS Operations Policies and Procedures

Definitions

1.11 See OPS-601, Appendix 1.

2. EXCEPTIONS

2.1 This policy **does not** regulate disclosures made:

i) to the Inspector General (IG) and the Security Intelligence Review Committee (SIRC) pursuant to their duties and functions;

ii) to the Secretariat of the Ministry of the Minister of Public Safety and Emergency Preparedness Canada pursuant to the Minister's responsibilities under the Act;

iii) in response to requests made under the *Access to Information Act* and the *Privacy Act*;

iv) to other Canadian Government institutions for the purposes of the Service's administrative requirements, e.g. Treasury Board, Auditor General, Library and Archives Canada.

3. PRINCIPLES

Legal requirements and Service policy

3.1 All Service disclosures of information obtained in the performance of its duties and functions must be authorized by in accordance with s. 19(2) or 19(2)(a) to (d) of the *CSIS Act*.

Protection of source and employee identity

3.2 Section 18(1) of the *CSIS Act* prohibits employees from disclosing any information from which can be inferred the identity of a past or present confidential source of information or assistance to the Service, or the identity of any past or present employee engaged in covert operational activities of the Service.

3.2.1 Such information may be disclosed in accordance with the conditions of s. 18(2) of the *CSIS Act*;

Assessment

3.3 When making disclosures, employees must take into consideration the potential threat to the security of Canada, the national interests, the privacy of the person(s) and organization(s) concerned and operational necessity.

3.3.1 Employees must also assess the impact of disclosure on:

- i) the safety of individuals;
- ii) human and technical sources;
- iii) investigative and collection techniques;
- iv) the third party rule;
- v) the possibility of disclosure through access to information legislation.

Discretion

3.4 In the course of operational activities, employees must exercise discretion and only disclose that information necessary to meet the Service's operational requirements.

4. RESPONSIBILITIES

Director

4.1 The Director is responsible for the reporting of security intelligence investigations involving holders of public office and for making disclosures in the public interest approved by the Minister pursuant to s. 19(2)(d) of the *CSIS Act*.

SECRET

Director's Secretariat

are responsible for the coordination or liaison between the Service and the Department.

Communications Branch

4.6 Communications Branch is responsible for answering public and media enquiries regarding specific operational activities of the Service, after consultation with the HQ operational branches.

5. GENERAL POLICY

Arrangements

5.1 Disclosures by the Service must comply with the conditions of arrangements or MOU entered with institutions of the Government of Canada, provincial agencies and governments, and foreign agencies.

5.1.1 When applicable, the persons authorized in these arrangements or MOUs will make the disclosures on behalf of the Service.

Requests

5.2 Requests from domestic or foreign agencies for information or intelligence must be justified under the Service's mandate.

5.2.1 If it appears the request cannot be justified under the mandate, the matter will be brought to the attention of _____ who will:

- i) seek additional information from the requesting agency, or
- ii) advise that the Service is not authorized to provide the requested information or intelligence.

Caveats

5.3 In order to control the subsequent use of information or intelligence disclosed by the Service, written disclosures to domestic or foreign agencies must be accompanied by appropriate caveats (OPS-603).

5.3.1 The Service may authorize, **in writing**, the original recipient(s) to further disclose Service information or intelligence to other parties.

Verbal disclosures

5.4 When making verbal disclosures, employees must sensitize the recipients to the confidentiality of the information or intelligence disclosed, and on the need to limit further dissemination.

5.4.1 Employees must record verbal disclosures in the appropriate file.

Reporting

5.5 For reasons of accountability and security, reports of disclosures must be placed on the appropriate operational file and contain such details as the identity of the recipient, circumstances of disclosure and the nature and extent of the information or intelligence disclosed.

5.5.1 Operational sectors must maintain a record of information or intelligence exchanged with domestic or foreign agencies.

NOTE: Refer to Information Management Branch (IM) procedures for the recording of disclosed s. 12 information i

SECRET

Privacy Impact Assessment

Canadian Security Intelligence Service
Operational Data Analysis Centre (ODAC)

DIRECTOR GENERAL/DIRECTEUR GÉNÉRAL


August 11, 2010
11 Août, 2010

COORDINATOR/ COORDONNATRICE
ACCESS TO INFORMATION AND PRIVACY /
ACCESS À L'INFORMATION ET PROTECTION
DES RENSEIGNEMENTS PERSONNELS

August 11, 2010
11 Août, 2010

CSIS POLICY: CONDUCT OF OPERATIONS

Secret

	Effective Date: 2014-01-10	Approved by: DDO	<u>French version</u>
	Policy Centre: DDO Sec	Supported by: Chief, DDO Sec	
	Version No: 1	File No: 305-3	
	Replaces: OPS-201 and OPS-801		

1. INTRODUCTION

Objective

- 1.1 The objective of this policy is to ensure the Service achieves its mission by conducting operations in a manner consistent with the Service's Policy Framework and the additional principles outlined in this policy.

Scope

- 1.2 This policy describes the Service's stance regarding operations conducted pursuant to its national security mandate pursuant to ss.12, 15 and 16 of the *Canadian Security Intelligence Service Act* (CSIS Act). It also provides additional principles and requirements that the Service and its employees will adhere to while working to achieve the commitments outlined in this policy.

Policy Centre

- 1.3 The Deputy Director of Operations (DDO) Secretariat is the policy centre for all matters related to the conduct of operations such as the use of operational tools and techniques, the application for and execution of warrant powers, and related policy documents.

Definitions

- 1.4 For definitions of specific terms used in this policy, readers should refer to the Policy Glossary.

Guidance and Information

- 1.5 Additional guidance and information (e.g. templates, forms, guides etc.) required to carry out this policy can be found on the DDO Secretariat's website. Links to procedures related to the use of specific operational tools and techniques to support operations can be found in the

2. PRINCIPLES

- 2.1 The Government and the people of Canada expect a high level of performance by the Service in its discharge of responsibilities under the *CSIS Act*. It is also expected that the Service will perform its duties and functions with due regard for the rule of law and respect for the rights and liberties as guaranteed under the *Charter of Rights and Freedoms*. Consequently, CSIS operations will be governed by the Service's Policy Framework, meaning that they will be **lawful** and **authorized, necessary, proportionate** and will represent an **effective** and **efficient** use of public resources.

CSIS POLICY: CONDUCT OF OPERATIONS

Secret

Lawful and Authorized

- 2.2 All CSIS Operations will comply with Canadian law and will be conducted pursuant to the Service's national security mandate as defined in ss.12, 15 and 16 of the *CSIS Act*.
- 2.3 Prior to conducting an operation, CSIS employees will obtain the appropriate approvals and for s.12 of the *CSIS Act* investigations, ensure that the appropriate targeting authority is in effect.
- 2.4 When there is uncertainty concerning the lawfulness of an operation, technique or action, employees are expected to consult with their supervisor for direction. Supervisors, in turn, may consult with their managers.

Necessary

- 2.5 The Service will conduct operations as necessary to fulfill its national security mandate and Government of Canada intelligence requirements pursuant to ss. 12, 15, and 16 of the *CSIS Act*. The collection of information and intelligence will be limited to that which is necessary for the purpose at hand, and is carried out only through such techniques as are necessary in the circumstances. The privacy of individuals will not be infringed unless there are valid reasons to do so, and then only to the extent that is necessary.

Proportionate

- 2.6 The Service's use of operational tools and techniques will be proportionate to the gravity and imminence of the threat being investigated. Additionally, the greater the risk associated with a particular activity, the higher the authority required to approve the activity.

Effective and Efficient Use of Public Resources

- 2.7 The Service will evaluate its operations to ensure that they are effective and that the resources dedicated to them are being used as efficiently as possible.

Safety of Employees and Public is Paramount

- 2.8 The Service will ensure during the planning and conduct of operations that potential risks to employees and/or members of the public are identified and mitigated to the extent possible.

Enhancing Future Capability

- 2.9 The Service will establish a mechanism to learn from our operational experiences to increase the efficiency of future operations. Service employees will be encouraged and expected to submit suggestions for improving operational tools.

Need to Know

- 2.10 Service employees will adhere to the "need-to-know" principle and mitigate the risk of unauthorized disclosure or compromise of classified information and assets.

CSIS POLICY: CONDUCT OF OPERATIONS

Secret

3. USE OF OPERATIONAL TOOLS AND TECHNIQUES

- 3.1 The operational tools and techniques available to the Service vary greatly and their use will depend on the nature of the potential threat. In general, the Service will use the least intrusive techniques first, except in emergency situations or where less intrusive investigative techniques would not be proportionate to the gravity and imminence of the threat, or if it appears they are unlikely to succeed.
- 3.1.1 The use of certain operational tools and techniques to support an operation conducted pursuant to s.12 of the *CSIS Act* will require a valid targeting authority. A list of operational tools and techniques and the targeting authority required for their use can be found in CSIS Procedures: Targeting.
- 3.2 The Service will establish procedures and approval authorities for requesting the use of operational tools and techniques. The level of authority required for approving the use of operational tools and techniques will be commensurate with their intrusiveness and with any risks associated to using them.

- 3.4 the Director will notify the Minister when there is a potential that a CSIS activity may have significant adverse impact on Canadian interests, such as:

- a) discrediting the Service or the GoC;
- b) giving rise to public controversy;
- c) a clear risk to human life;
- d) affecting domestic interdepartmental or intergovernmental relations;
- e) affecting Canadian relations with any country or international organization of states; and/or
- f) contravening any of the directives with respect to the management of the Service in existing Ministerial Direction or a policy.

CSIS POLICY: CONDUCT OF OPERATIONS

Secret

Execution of Warrant Powers

- 3.6 The execution of warrant powers is considered an operational tool that the Service may use to further an investigation into a threat to the security of Canada, to perform its duties and functions under s.16 of the *CSIS Act*,
- 3.7 When executing warrant powers the Service will comply with the terms and conditions contained in the warrant and with any additional direction issued by the Federal Court and/or the Minister of Public Safety.
- 3.8 The Service recognizes that there is a heightened risk or potential for controversy given the intrusiveness of some warrant powers. To minimize this risk, the decision to execute warrant powers will be based on the principles outlined in this policy and will be made following established procedures.

Warrant Acquisition and Coordination

- 3.9 Service employees will employ rigour while engaging in the warrant or production order acquisition process to ensure accuracy and completeness, and that sources of information are not inadvertently disclosed in the application for a warrant.
- 3.10 The Warrant Acquisition, Control and Requirements (WACR) unit of the DDO Secretariat will be responsible for the overall coordination of Service's Federal Court warrant applications. To reflect the importance of warrants in regards to furthering investigations, WACR will develop and continually review warrant acquisition best practices and procedures to ensure effectiveness and efficiency. The unit will ensure that required documentation in support of the application is prepared and reviewed prior to filing the warrant application with the Court.

Warrant Committees

- 3.11 The Warrant Review Committee (WRC), chaired by the Director, will be responsible for ensuring that the application for a warrant is both necessary and proportionate and that if the warrant is granted, its execution would constitute an effective and efficient use of the Service's resources.
- 3.12 The DDO Review Committee, chaired by the Chief, DDO Secretariat, will be responsible for reviewing the affidavit and exhibits
to ensure the documents are consistent with Ministerial Direction, Service standards, and the principles outlined in this policy before the warrant application is filed.

Pretexts

- 3.13 While in certain circumstances, parallel investigations might be necessary (for example investigations mandated in accordance with ss. 12, 15, or 16 of the *CSIS Act*), operations conducted to support an investigation under one section of the *CSIS Act* will not be used as a pretext for conducting operations pursuant to another section of the *Act*.

CSIS POLICY: CONDUCT OF OPERATIONS

Secret

Use of information collected pursuant to s.15 of the *CSIS Act*

- 3.14 The Service may use information, collected pursuant to s.15 of the *CSIS Act*, to the extent that it is necessary to support specific investigations pursuant to s.12 of the *CSIS Act*.

4. COOPERATION WITH CANADIAN AND FOREIGN AGENCIES

4.1

To facilitate this cooperation, the Service may enter into arrangements with Canadian and foreign partners in accordance with s.17 of the *CSIS Act*, Ministerial Direction and the principles outlined in this policy.

- 4.1.1 In emergency circumstances where no s.17 of the *CSIS Act* arrangement exists, the Service may undertake whatever exchanges or cooperation as are necessary. In these cases, the Service will advise the Deputy Minister of Public Safety as soon as possible.

Joint Operations

- 4.2 The Service considers a joint operation to be an activity that seeks to advance an investigation of mutual interest to the participants by combining resources and sharing the product.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

CSIS POLICY: CONDUCT OF OPERATIONS

Secret

Operational Assistance

- 4.8 The Service considers Operational Assistance as an activity undertaken by the Service on behalf of a requesting organization, or vice versa,

Foreign Operational Activity

- 4.14 In addition to complying with the principles outlined in this policy, CSIS operational activities conducted outside Canada will:
- a) hold potential benefit for Canada and its national interests;
 - b) be considered for their impact on Canadian foreign policy interests and objectives; and

CSIS POLICY: CONDUCT OF OPERATIONS

Secret

5. INDIVIDUALS AND ORGANIZATIONS DEEMED OF SPECIAL CONSIDERATION

- 5.1 The Service will weigh the need to use intrusive operational tools and techniques against potential damage to civil liberties or the activities of a Canadian Fundamental Institution (CFI). CFIs include, but are not limited to, post-secondary, political, religious and media institutions.

6. EMPLOYEE CONDUCT

- 6.1 CSIS Employees are expected to conduct themselves in a manner consistent with the Service's Code of Conduct and the following standards during the performance of their duties:

- a) their actions will be impartial and in compliance with the *CSIS Act* and established CSIS procedures;
- b) their deportment will be professional, courteous and respectful when dealing with the public;

CSIS POLICY: CONDUCT OF OPERATIONS

Secret

- c) they will be discreet, apply the need-to-know principle, and abide by established standards of security during the performance of their duties and functions so that sensitive sources of information, collection programs and operational methodologies are not compromised;
- d) they will report in a timely, accurate, complete and objective manner all information pertinent to a collection program;
- e) they will clearly distinguish between fact, analysis, and opinion in their reports; and
- f) they will refrain from offering personal opinions on sensitive issues which could lead to unnecessary confrontation or controversy.

6.2

Unlawful Activity

- 6.3 When an employee learns of unlawful activity during the performance of his or her duties and functions, he or she will advise his/her supervisor or manager as soon as possible. The employee may also make an internal disclosure in accordance with ADM-406, "Internal Disclosure of Wrongdoing and Reprisal Protection" to the Senior Officer of Disclosure of Wrongdoing.

7. REPORTING AND RETENTION OF OPERATIONAL INFORMATION AND MATERIALS

- 7.1 All information, intelligence and materials collected during an operation will be reported and retained in accordance with the Service's existing policies and procedures for reporting and retaining operational information and materials.

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION